

IN THE UNITED STATES DISTRICT COURT
FOR WESTERN DISTRICT OF NORTH CAROLINA CHARLOTTE DIVISION

IN THE MATTER OF THE SEARCH OF
“DEVICES” as per Attachment A,
CURRENTLY LOCATED AT
7915 Microsoft Way,
Charlotte, North Carolina 28273

Case No. _____

AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE

I, Scott Atwood, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an Application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation, hereinafter FBI, and have been since September 2007. In my current capacity, I am assigned to investigate federal crimes against children to include international parental kidnapping, child abductions, sexual exploitation of children, domestic trafficking of children/prostitution, child sex tourism and national sex offender registry violations. I have conducted numerous investigations involving a number of sophisticated investigative techniques as well as follow on training as it relates to my current assignment. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. This Affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched is 1) an iPhone Model Product Red; 2) an iPhone Model A1549, IMEI 354449067955568; 3) an iPhone Model A1303, IC ID 579C-A1303A; 4) an iPhone Model A1387, IC 579C-E2430A; 5) a WD My Passport Ultra External Drive, SN WX21E54UX486; 6) a Seagate Backup Plus 4TV External Drive, SN NA7TXA6D; 7) a HP Pavilion Model p7-1074; 8) an iMac Core i5 with power cord; 9) a Transcend 4GB thumb drive; 10) a SanDisk 64GB micro-SD card with adapter; 11) a GoPro Hero 4 with SanDisk 64GB micro-SD card; 12) a silver thumb drive with “Essex Home” label; 13) an iPad model A1458; 14) an Apple MacBook Pro laptop, serial number C02PFR7WVH5; 15) a Touro University flash drive; 16) a Medical College of Wisconsin flash drive in the shape of a key; 17) a Seagate Ultra Touch 2TB external drive, serial number NAB20C38, hereinafter the “Devices.” The aforementioned devices are currently located at the Charlotte Division of the FBI under the control of the Evidence Custodian.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of 18 U.S.C. § 2252A, relating to material involving the sexual exploitation of minors.

a. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing, or accessing with intent to view, any book, magazine, periodical, film,

videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce , or in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:

a. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

b. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

e. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

f. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person. For the purposes of 18 U.S.C. § 2256(8)(B), “sexually explicit conduct” means (i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (ii) graphic or lascivious simulated: (I) bestiality; (II) masturbation; or (III) sadistic or masochistic abuse; or (iii) graphic or simulated lascivious exhibition of the anus, genitals, or pubic area of any person.

g. “URL” is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

h. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means

which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

i. “Identifiable minor” (A) means a person-- (i)(I) who was a minor at the time the visual depiction was created, adapted, or modified; or (II) whose image as a minor was used in creating, adapting, or modifying the visual depiction; and (ii) who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic, such as a unique birthmark or other recognizable feature; and (B) shall not be construed to require proof of the actual identity of the identifiable minor.

j. “Graphic”, when used with respect to a depiction of sexually explicit conduct, means that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted.

k. “Indistinguishable” used with respect to a depiction, means virtually indistinguishable, in that the depiction is such that an ordinary person viewing the depiction would conclude that the depiction is of an actual minor engaged in sexually explicit conduct. This definition does not apply to depictions that are drawings, cartoons, sculptures, or paintings depicting minors or adults.

PROBABLE CAUSE

8. On September 22, 2021, KIMBERLY TATUM, hereinafter KIMBERLY, wife of DAVID TATUM, hereinafter TATUM, provided the following information to FBI agents:

9. KIMBERLY and TATUM have an Apple Mac laptop computer, hereinafter MAC, which is jointly utilized by KIMBERLY and TATUM. TATUM is employed as an Adolescent and Adult Psychiatrist in Charlotte, North Carolina. TATUM utilizes the MAC in order to maintain patient records and carries it to and from work on a regular basis. Along with the MAC, TATUM also carries two (2) external hard drives in the same computer bag when traveling to and from work.

10. In August 2021, KIMBERLY observed several photographic images of young children stored in a folder on the desktop of the MAC. The images were of young girls approximately 10 years old and included the words “teen gallery.” Several photographs depicted young girls with clothes on and fully nude. While on the Safari application, KIMBERLY observed an open internet window to what she described as an artificial intelligent, deep fake website. According to KIMBERLY, this website could take a photograph of a clothed person and make the person appear nude. While utilizing the MAC, KIMBERLY observed several photographs of young girls, including approximately 10 nude images of young girls, one of which had her legs spread fully exposing her genitalia. KIMBERLY took photographs and videos of what she observed from the MAC and copied said photographs and videos onto a flash drive. KIMBERLY provided the FBI with the flash drive containing, but not limited to, the aforementioned photographs and videos.

11. In approximately the summer of 2021, KIMBERLY observed, on at least one occasion, an external hard drive attached to the MAC. The external drive was described as a “My Passport” hard drive. Recently, TATUM purchased a new external hard drive from Costco. This hard drive was described as a Seagate hard drive.

12. On September 22, 2021, KIMBERLY, during the voluntarily meeting with FBI agents, provided FBI agents with the following items: 1) an iPhone Model Product Red; 2) an iPhone Model A1549, IMEI 354449067955568; 3) an iPhone Model A1303, IC ID 579C-A1303A; 4) an iPhone Model A1387, IC 579C-E2430A; 5) a WD My Passport Ultra External Drive, SN WX21E54UX486; 6) a Seagate Backup Plus 4TV External Drive, SN NA7TXA6D.

- a. 1) iPhone Model Product Red was described as a red iPhone 8. This was the most recent phone TATUM was known to utilize prior to his current cellular telephone.
- b. 2) iPhone Model A1549, IMEI 354449067955568 was described by KIMBERLY as an iPhone 6 with a green case which TATUM utilized circa 2014-2016.
- c. 3) iPhone Model A1303, IC ID 579C-A1303A and 4) iPhone Model A1387, IC 579C-E2430A were described by KIMBERLY as older phones which TATUM utilized before 2014.
- d. 5) WD My Passport Ultra External Drive, SN WX21E54UX486 was described by KIMBERLY as an external drive which was originally her drive which she used to backup her laptop from Grad School. The password hint on the drive was bees. KIMBERLY believed this drive to be the same drive which TATUM carried in the bag along with the MAC.
- e. 6) Seagate Backup Plus 4TV External Drive, SN NA7TXA6D was described by KIMBERLY as a blue external drive which was not password protected.

13. On September 22, 2021, Affiant reviewed the aforementioned flash drive previously provided to the FBI by KIMBERLY. A review of the flash drive revealed the following:

14. A recorded video, IMG_6667.MOV, begins with the MAC opened and operational. The mouse moved to the Safari application and a browser window was opened. The website observed was www.deepsukebe.io/en/.¹ A second tab was also observed as titled “private browsing.”

15. A recorded video, IMG_6640.MOV begins with the MAC opened and operational. An opened image of a nude girl (JBGhy49t6rjsf.jpg), hereinafter Image 1, believed to be under the age of 15, was observed in the upper left-hand corner of the screen. The girl appeared to be talking on a cellular telephone while sitting with her legs spread in a lewd and lascivious manner, exposing genitalia. The breasts were also fully exposed. An open folder titled “Downloads” was also observed in the home screen background. In the open folder, a similar image, hereinafter Image 2, was observed depicting the same girl in Image 1, except she was fully clothed.

16. A recorded video, IMG_6642.MOV, begins with the MAC opened and operational. A folder labeled “CPT” was opened to reveal 14 total images, two of which depicted nude girls believed to be under the age of 15. In addition to Image 2, an image (JBGgx18k7dtcp copy.jpg), hereinafter Image 3, was observed of a nude girl believed to be under the age of 15. In Image 3, the girl was sitting on the side of a swimming pool with breasts fully exposed. Her legs were crossed semi-exposing her pubic area. The words “teengallery” were observed in the lower right-hand corner of Image 3. In addition, image (JBGgx18k7dtcp.jpg), hereinafter Image 4, was observed of the same girl in the same pose, sitting poolside wearing a gray swimsuit. The term

¹ According to the deepsukebe.io website, the site is an AI-leveraged nudifier used to turn your photo to a nudified photo, revealing the truth hidden under clothing. Deepsukebe claims to generate the most natural and authentic images, equipped with state-of-the-art artificial intelligence created by scientist. The site further claims it is more powerful than deepnude variants and can handle a diverse range of clothing and women.

“teengallery.com” was observed in the lower right-hand corner of Image 4. Another image (JBGzp5c2n9xm0copy.jpg), hereinafter image 5, was observed of a naked girl believed to be under the age of 15. In Image 5, the girl was standing, wearing a pink hat and was fully nude exposing breasts and genital area from the front. The term “teengallery.com” was observed in the lower right-hand corner of Image 5. A recorded video, IMG_6654.MOV, begins with the MAC opened and operational. A window titled “Recents” is opened on the home screen. An image (JBGfcmvsn42t7copy.jpg), hereinafter Image 6, was observed of a nude girl believed to be under the age of 15. In Image 6, the girl was standing fully nude exposing breasts and genital area from the front. The term “teengallery.com” was observed in the lower right-hand corner of Image 6. Images 1, 3 and 5 were also observed in the open window.

17. A review of images on the flash drive depicted approximately seven images of nude girls under the age of 15. At least one photograph, Image 1, showed a nude girl with her legs spread, fully exposing the breasts and genitalia. One image labeled IMG_6655.jpg, hereinafter Image 7, depicted five girls believed to be under the age of 15, standing side-by-side whom were fully clothed. Image labeled IMG_6657.jpg, hereinafter Image 8, depicted four out of the five girls viewed in Image 6, fully nude exposing the breasts and pubic area. Pubic hair was observed on at least one of the girls. A separate image labeled IMG_6607.jpg, hereinafter Image 9, depicted Image 8 on what was believed to be a cellular telephone screen. The background of Image 9 was believed to be from the website deepsukebe.io and also contained a digital time clock in the upper left-hand corner of the phone screen and the term 5G in the upper right-hand corner of the phone screen.²

² Your Affiant and AUSA Cortney Randall met with U.S. Magistrate Judge Cayer and made a copy of the images and videos described in this Affidavit for his review.

18. On September 22, 2021, FBI agents traveled to the residence of KIMBERLY and DAVID TATUM, [REDACTED] Agents contacted KIMBERLY TATUM at the residence and requested a consent search of the residence in order to locate digital storage devices which could be used to store images depicting child pornography. Agents requested KIMBERLY TATUM's assistance in identifying common areas in the residence which may contain digital storage devices. During the consensual search, FBI agents seized the following items: 7) a HP Pavilion Model p7-1074; 8) an iMac Core i5 with power cord; 9) a Transcend 4GB thumb drive; 10) a SanDisk 64GB micro-SD card with adapter; 11) a GoPro Hero 4 with SanDisk 64GB micro-SD card; 12) a silver thumb drive with "Essex Home" label; 13) an iPad model A1458.

- a. 7) The HP Pavilion Model p7-1074; 8) an iMac Core i5 with power cord; 9) a Transcend 4GB thumb drive; 10) a SanDisk 64GB micro-SD card with adapter; 11) a GoPro Hero 4 with SanDisk 64GB micro-SD card; 12) a silver thumb drive with "Essex Home" label were seized from an office inside the residence.

KIMBERLY advised Agents that both KIMBERLY and TATUM use the office.

- b. 13) The iPad model A1458 was seized from the upstairs bedroom shared by KIMBERLY and TATUM.

19. On September 22, 2021, FBI Agents located TATUM in a parking garage near his place of employment in Charlotte, North Carolina. Agents requested to speak with TATUM and asked to see his laptop computer. TATUM informed Agents that he left the computer at his house and requested to return to his residence and speak with Agents. Prior to departing the parking garage, Agents requested a voluntary search of TATUM's vehicle, a Tesla Model 3,

North Carolina license plate FFF3313, to which TATUM voluntarily agreed. During the voluntary search, Agents observed TATUM remove a small bag from the front passenger's seat. When asked of the contents of the bag, TATUM informed Agents he forgot his laptop was in the bag. Agents informed TATUM the bag was subject to seizure and requested to speak with TATUM about the laptop. TATUM voluntarily agreed to speak with Agents in their FBI vehicle which was parked nearby. During the interview, TATUM provided the following information:

20. TATUM had a MacBook laptop computer which he used to manage patient records, of which 75 percent are children. TATUM had a user profile on the laptop which was password protected. KIMBERLY also used the same user profile and accessed the profile using the same password. TATUM obtained images of teen girls from a website called "teen gallery." When TATUM saw a girl whom he thought was attractive, TATUM would input the image in a "deep fake" website which would make the girl in the image appear nude. TATUM advised he first used deep fake websites about four to five years ago. TATUM was asked if the girls he input in the deep fake website were over the age of 18, to which TATUM responded, "it's it's possible but questionable. I'm sorry." When asked if any reasonable person would think the images in question were of a persons under the age of 18 or under the age of 13, TATUM responded, "I don't think any reasonable person would think they are under the age of 13. I think it's possible people might think under the age of 18 is possible. But I didn't go and go and like I don't know what their ages are." TATUM admitted he masturbated to a photograph of an ex-girlfriend, when she was a minor, which TATUM input on the deep fake website resulting in a nude image of the ex-girlfriend. TATUM further admitted to saving these images to zip drives or thumb drives which were unencrypted and stored at his office at home. When asked about external storage devices, TATUM advised he stored pornography on drives.

21. During the interview, TATUM was asked if he owned any external hard drives used to store digital media. TATUM advised FBI Agents of an external drive inside his Tesla sedan. Affiant asked TATUM if TATUM could retrieve the external drive from the Tesla. TATUM verbally agreed to retrieve the external drive from the Tesla and subsequently provided the drive to Affiant. This drive was determined to be a Seagate Ultra Touch 2TB external drive, serial number NAB20C38.

22. At the conclusion of the interview, TATUM requested his wallet and medication from the bag which contained the laptop computer. Affiant opened the bag to provide TATUM with his requested items. Upon looking in the bag for TATUM's wallet and medication, Affiant observed an Apple laptop computer and one key shaped flash drive. Subsequently, all items were removed from the bag and one additional flash drive was observed. Personal items were returned to the bag and the bag was given to TATUM prior to his departure.

23. Prior to his departure, the following items were seized from TATUM: 14) an Apple MacBook Pro laptop, serial number C02PFR7WVH5; 15) a Touro University flash drive; 16) a Medical College of Wisconsin flash drive in the shape of a key; 17) a Seagate Ultra Touch 2TB external drive, serial number NAB20C38.

24. The Devices are currently in storage at the Charlotte Division of the FBI, 7915 Microsoft Way, Charlotte, North Carolina, 28273. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the FBI.

TECHNICAL TERMS

25. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable

storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- e. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed

properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

26. Based on my training, experience, and research, I know that the Devices have capabilities that allow it to serve as a wireless telephone, digital camera, portable media player. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

27. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the devices. This information can sometimes be recovered with forensics tools.

28. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file

on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the

application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to create, access or possess child pornography, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

31. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve

the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

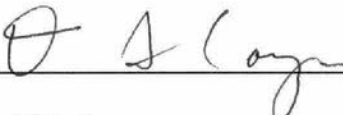
32. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

/s/ Scott Atwood_____
Special Agent
Federal Bureau of Investigation

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 30th day of September, 2021, at 2:24 PM

Signed: September 30, 2021



David S. Cayer
United States Magistrate Judge



ATTACHMENT A

DESCRIPTION OF THE PREMISES TO BE SEARCHED

1. The property to be searched is 1) an iPhone Model Product Red; 2) an iPhone Model A1549, IMEI 354449067955568; 3) an iPhone Model A1303, IC ID 579C-A1303A; 4) an iPhone Model A1387, IC 579C-E2430A; 5) a WD My Passport Ultra External Drive, SN WX21E54UX486; 6) a Seagate Backup Plus 4TV External Drive, SN NA7TXA6D; 7) a HP Pavilion Model p7-1074; 8) an iMac Core i5 with power cord; 9) a Transcend 4GB thumb drive; 10) a SanDisk 64GB micro-SD card with adapter; 11) a GoPro Hero 4 with SanDisk 64GB micro-SD card; 12) a silver thumb drive with “Essex Home” label; 13) an iPad model A1458; 14) an Apple MacBook Pro laptop, serial number C02PFR7WVH5; 15) a Touro University flash drive; 16) a Medical College of Wisconsin flash drive in the shape of a key; 17) a Seagate Ultra Touch 2TB external drive, serial number NAB20C38, hereinafter the “Devices.” The aforementioned devices are currently located at the Charlotte Division of the FBI under the control of the Evidence Custodian.

2. This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

ITEMS TO BE SEARCHED AND SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18 U.S.C. § 2252A(a)(5)(B):

1. All records on the Devices described in Attachment A that relate to violations of Title 18, United States Code, Section 2252A(a)(5)(B) relating to possession of, or access with intent to view, child pornography, to include:

- a) Child pornography;
- b) Child erotica;
- c) Visual depictions used to generate child pornography or child erotica;
- d) Information, correspondence, records, documents or other materials constituting evidence of or pertaining to child pornography or child erotica, or constituting evidence of or pertaining to the possession or accessing through interstate or foreign commerce of child pornography, child erotica, or visual depictions of minors used to generate child pornography or child erotica, or constituting evidence of or pertaining to an interest in child pornography or sexual activity with children;
- e) Records or documents evidencing occupancy or ownership of the DEVICES, including utility and telephone bills, email or addressed correspondence;

- f) Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved and location of occurrence;
 - g) Records and information referencing or revealing the use of remote computing services such as email, cloud storage or online social media services; and
- 2) For the computer or storage medium whose seizure is otherwise authorized by this warrant (hereinafter, "DEVICES"):
 - (a) evidence of who used, owned, or controlled the DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - (b) evidence of software that would allow others to control the DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - (c) evidence of the lack of such malicious software;
 - (d) evidence of the attachment to the DEVICES of other storage devices or similar containers for electronic evidence;
 - (e) evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the DEVICES;
 - (f) evidence of the times the DEVICES was used;

(g) records of or information about Internet Protocol addresses used by the DEVICES;

(h) records of or information about the DEVICES's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

(i) contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

If the government identifies seized materials, that are potentially attorney-client privileged or

subject to the work product doctrine (“protected materials”), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team will review seized communications and segregate potentially protected materials, i.e. communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team concludes that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team.